The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
9/14/2010

SUBJECT:
Vulnerability in Remote Procedure Call Could Allow Remote Code Execution (MS10-066)

OVERVIEW:
A vulnerability has been discovered in the way Microsoft Windows handles a specially crafted RPC response. Remote Procedure Call (RPC) is a protocol that one program can use to request a service from a program located in another computer on a network. This vulnerability may be exploited by sending a specially crafted RPC response. Successful exploitation will result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

Windows XP
Windows Server 2003

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability has been discovered in the way Microsoft Windows handles a specially crafted RPC response. Remote Procedure Call (RPC) is a protocol that one program can use to request a service from a program located in another computer on a network. This vulnerability may be exploited by sending a specially crafted RPC response to a client-initiated RPC request. The vulnerability is caused due to a memory allocation error in the parsing of RPC responses. Successful exploitation will result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

- Block ports associated with RPC at the network boundary unless there is a documented business need.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/bulletin/MS10-066.mspx

Securityfocus:
http://www.securityfocus.com/bid/43119

Secunia:
http://secunia.com/advisories/41412

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2567